PATENT ABSTRACTS OF JAPAN

(11)Publication number : 10-302034

(43)Date of publication of application : 13.11.1998

(51)Int.Cl. G06K 17/00
G06T 7/00
G06K 19/10

(21)Application number : 09-107101

(22)Date of filing : 24.04.1997

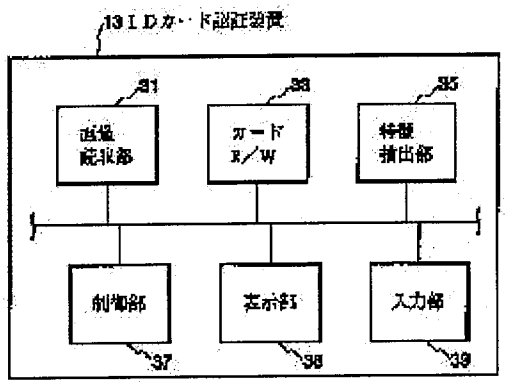
(71)Applicant : N T T DATA:KK

(72)Inventor : ARAKAWA HIROKI
IWAMOTO HIROKI

(54) AUTHENTICATION SYSTEM, CARD ISSUING DEVICE, AUTHENTICATION DEVICE, CARD FOR AUTHENTICATION AND AUTHENTICATION METHOD

(57)Abstract:

PROBLEM TO BE SOLVED: To detect a forged unauthorized card by storing feature data in the magnetic storage part of a card for authentication and collating data read from the magnetic storage part with the data generated by extracting features from image information.



SOLUTION: The image read part 31 of an ID card authentication device 13 is constituted of an image scanner or the like for instance, reads a photograph (image) stuck to the photograph sticking part of an ID card and obtains image data. A card reader/writer 33 writes the data to a magnetic stripe or reads the data stored on the magnetic stripe. Also, a feature extraction part 35 extracts the feature data for specifying the image data from the obtained image data. Then, at the time of authenticating the ID card, a control part 37 compares the data stored on the magnetic stripe with the feature data extracted from the photograph stuck to the photograph sticking part of the ID card of an authentication object and checks the propriety of the ID card.

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A card for attestation characterized by comprising the following which picture information which specifies a user is displayed and is provided with a storage parts store, Are an authentication device which processes this card for attestation an authentication system which it has, and said authentication device, At a card issuing means provided with a reading means which reads said picture information currently displayed on said card for attestation, a feature extraction means which extracts the feature from said picture information read by said reading means, and generates characteristic data, and a writing means which writes said characteristic data in said storage parts store, and the time of attestation.
A creating means which reads said picture information currently displayed on said card for attestation by said reading means, and generates characteristic data by said feature extraction means.
A reading means which reads said characteristic data currently written in said storage parts store of said card for attestation by said writing means.
Said characteristic data read from said reading means.
Said characteristic data generated by said creating means.
A discriminating means which distinguishes whether it ****** or not.
Said characteristic data read from said reading means.
A means to notify detection of a wrong card when said characteristic data and ** which were generated by said creating means were not in agreement and it is distinguished.

[Claim 2]A card issuing device characterized by comprising the following in an authentication system which attests a user using a card for attestation which picture information which specifies a user is displayed and is provided with a storage parts store.
A reading means which reads said picture information as which said card issuing device is

beforehand displayed on said card for attestation.
A feature extraction means which extracts the feature from said picture information read by said reading means, and generates characteristic data, and a writing means which writes said characteristic data in said storage parts store.

[Claim 3]An authentication device which attests a card for attestation provided with a storage parts store characteristic data which picture information which specifies a user was displayed, and extracted and generated the feature from this picture information is remembered to be, comprising:
A reading means which reads said picture information as which said authentication device is displayed on said card for attestation.
A feature extraction means which extracts the feature from said picture information read by said reading means, and generates characteristic data.
A reading means which reads said characteristic data currently written in said storage parts store of said card for attestation.
Said characteristic data read by said reading means and said characteristic data generated by said feature extraction means, A means to notify detection of a wrong card when a discriminating means which distinguishes whether it ****** or not, said characteristic data read by said reading means, said characteristic data generated by said feature extraction means, and ** were not in agreement and it is distinguished.

[Claim 4]A card for attestation characterized by comprising the following used in an authentication system which attests a user.
A viewing area as which said card for attestation displays picture information which specifies a user.
A storage area which memorizes characteristic data which extracted the feature from said picture information currently displayed on said viewing area, and was generated.

[Claim 5]An authentication method which attests a user using a card for attestation which picture information which specifies a user is displayed and is provided with a storage parts store, comprising:
A reading step which reads said picture information currently beforehand displayed on said card for attestation.
A feature extraction step which extracts the feature from said read picture information, and generates characteristic data, and a memory step which memorizes said characteristic data generated from said feature extraction step to said storage parts store of said card for attestation.

[Claim 6]An authentication method which picture information which specifies a user is displayed and attests a user using a card for attestation provided with a storage parts store characteristic data which extracted and generated the feature is remembered to be from this picture information, comprising:
A reading step which reads said picture information currently beforehand displayed on said card for attestation.
A feature extraction step which extracts the feature from said picture information read by the aforementioned reading step, and generates characteristic data.
A read-out step which reads said characteristic data beforehand memorized by said storage parts store of said card for attestation.
Said characteristic data read by the aforementioned read-out step and said characteristic data generated by said feature extraction step, A step which notifies detection of a wrong card when a discriminating step which distinguishes whether it ****** or not, said characteristic data read by the aforementioned read-out step, said characteristic data generated by said feature extraction step, and ** were not in agreement and it is distinguished.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention relates to the authentication system which attests a user.
[0002]
[Description of the Prior Art]It is necessary to check that the photograph stuck is not stuck again unjustly in the authentication system using the ID card etc. in which the user's photograph is stuck. For this reason, for example, the image data of the stuck photograph is memorized to an ID card, and the authentication system which attests by comparing them is proposed.
[0003]
[Problem(s) to be Solved by the Invention]In such a system, the system which uses the image data of the stuck photograph as data memorized by the ID card, for example is proposed. In this case, since data volume was great, it is impossible to use a storage with a small storage capacity of a magnetic stripe etc., and mass IC (Integrated Circuit) memory needed to be used.
[0004]For this reason, the image data of a photograph is compressed and the system which memorizes the compressed data which made data volume small to an ID card is also proposed. However, in that authenticating processing, there was a problem that a parenchyma top was difficult for checking that the data which elongated the compressed data beforehand memorized by the card, the image data of the photograph stuck, and ** are in agreement, in this case. The data compressed and elongated is because the data before compression is not thoroughly in agreement in many cases.
[0005]As these proposed measures, for example to JP,8-129634,A. The photograph stuck is read at the time of attestation, and it compresses in the same procedure as the compressed data beforehand memorized by the card, and also elongates, and the system which compares

the data obtained as a result and the data which elongated the compressed data memorized by the card is proposed. However, the data memorized by the card is elongated in this case at the time of attestation, and the image data of the photograph stuck on the card must be compressed, it must elongate, and there is a problem that a response becomes late.

[0006]This invention was made in view of the above-mentioned actual condition, and an object of this invention is for forgery to provide the authentication system, device, and method using an ID card easy [composition] and cheap and this ID card difficult. It sets it as other purposes to use for these furthermore and to provide a suitable card issuing device and the card for attestation.

[0007]

[Means for Solving the Problem]In order to attain the above-mentioned purpose, an authentication system concerning the 1st viewpoint of this invention, Are a card for attestation which picture information which specifies a user is displayed and is provided with a storage parts store, and an authentication device which processes this card for attestation an authentication system which it has, and said authentication device, A reading means which reads said picture information currently displayed on said card for attestation, In a card issuing means provided with a feature extraction means which extracts the feature from said picture information read by said reading means, and generates characteristic data, and a writing means which writes said characteristic data in said storage parts store, and the time of attestation, A creating means which reads said picture information currently displayed on said card for attestation by said reading means, and generates characteristic data by said feature extraction means, A reading means which reads said characteristic data currently written in said storage parts store of said card for attestation from said writing means, Said characteristic data read from said reading means, and said characteristic data generated by said creating means, An authentication means provided with a means to notify detection of a wrong card when a discriminating means which distinguishes whether it ****** or not, said characteristic data read from said reading means, said characteristic data generated by said creating means, and ** were not in agreement and it is distinguished, ********.

[0008]According to such composition, characteristic data which extracted and generated the feature from picture information which specifies a user is memorized to a storage parts store, and data read from a storage parts store and data which carried out feature extraction and was generated from picture information are compared at the time of attestation. A wrong card forged by unjust change of picture information, such as **** of a photograph, thereby, for example is detectable. Since data volume memorized on a card by extracting only the feature from picture information becomes a small quantity, a card for attestation is realizable using a magnetic storage medium etc. in which it is cheap and structure is easy.

[0009]A card issuing device concerning the 2nd viewpoint of this invention, Using a card for

attestation which picture information which specifies a user is displayed and is provided with a storage parts store, are a card issuing device in an authentication system which attests a user, and said card issuing device, It has a reading means which reads said picture information currently beforehand displayed on said card for attestation, a feature extraction means which extracts the feature from said picture information read by said reading means, and generates characteristic data, and a writing means which writes said characteristic data in said storage parts store.

[0010]According to such composition, characteristic data which extracted and generated the feature from picture information which specifies a user is memorized to a storage parts store as data for collation at the time of attestation. Thereby for example, forgery of a card by unjust change of picture information, such as **** of a photograph, can be prevented. Since data volume memorized on a card by extracting only the feature from picture information becomes a small quantity, a card for attestation is realizable using a magnetic storage medium etc. in which it is cheap and structure is easy.

[0011]An authentication device concerning the 3rd viewpoint of this invention, It is an authentication device which attests a card for attestation provided with a storage parts store characteristic data which picture information which specifies a user was displayed, and extracted and generated the feature from this picture information is remembered to be, A reading means which reads said picture information as which said authentication device is beforehand displayed on said card for attestation, A feature extraction means which extracts the feature from said picture information read by said reading means, and generates characteristic data, A reading means which reads said characteristic data currently written in said storage parts store of said card for attestation, Said characteristic data read by said reading means and said characteristic data generated by said feature extraction means, When a discriminating means which distinguishes whether it ****** or not, said characteristic data read by said reading means, said characteristic data generated by said feature extraction means, and ** were not in agreement and it is distinguished, it has a means to notify detection of a wrong card.

[0012]According to such composition, data which was read from a storage parts store and which extracted the feature beforehand and was generated, and data which carried out feature extraction and was generated from picture information are compared at the time of card authentication. A wrong card forged by unjust change of picture information, such as **** of a photograph, thereby, for example is detectable.

[0013]A card for attestation concerning the 4th viewpoint of this invention, It is a card for attestation used in an authentication system which attests a user, and said card for attestation is provided with a storage area which memorizes characteristic data which extracted the feature from a viewing area which displays picture information which specifies a user, and said

picture information currently displayed on said viewing area, and was generated.
[0014]According to such composition, this card for attestation is provided with a storage area for memorizing characteristic data which extracted and generated the feature from picture information which specifies a user as data for collation at the time of attestation. Thereby for example, forgery of a card by unjust change of picture information, such as **** of a photograph, can be prevented. Since data volume memorized on a card by extracting only the feature from picture information becomes a small quantity, a card for attestation is realizable using a storage with an easy structure, etc.
[0015]An authentication method concerning the 5th viewpoint of this invention, A reading step which reads said picture information which picture information which specifies a user is displayed, and is an authentication method which attests a user using a card for attestation provided with a storage parts store, and is displayed on said card for attestation, The feature is extracted from said read picture information, and it has a feature extraction step which generates characteristic data, and a memory step which memorizes said characteristic data generated from said feature extraction step to said storage parts store of said card for attestation.
[0016]According to such composition, characteristic data which extracted and generated the feature from picture information which specifies a user is memorized to a storage parts store of a card for attestation as data for collation at the time of attestation. Thereby for example, forgery of a card by unjust change of picture information, such as **** of a photograph, can be prevented. Since data volume memorized on a card by extracting only the feature from picture information becomes a small quantity, a card for attestation is realizable using a storage etc. in which it is cheap and structure is easy.
[0017]An authentication method concerning the 6th viewpoint of this invention, It is an authentication method which picture information which specifies a user is displayed and attests a user using a card for attestation provided with a storage parts store characteristic data which extracted and generated the feature is remembered to be from this picture information, A reading step which reads said picture information currently beforehand displayed on said card for attestation, A feature extraction step which extracts the feature from said picture information read by the aforementioned reading step, and generates characteristic data, A read-out step which reads said characteristic data beforehand memorized by said storage parts store of said card for attestation, Said characteristic data read by the aforementioned read-out step and said characteristic data generated by said feature extraction step, When a discriminating step which distinguishes whether it ****** or not, said characteristic data read by the aforementioned read-out step, said characteristic data generated by said feature extraction step, and ** were not in agreement and it is distinguished, it has a step which notifies detection of a wrong card.

[0018]According to such composition, data which was read from a storage parts store and which extracted the feature beforehand and was generated, and data which carried out feature extraction and was generated from picture information are compared at the time of card authentication. A wrong card forged by unjust change of picture information, such as **** of a photograph, thereby, for example is detectable.

[0019]

[Embodiment of the Invention]The authentication system concerning an embodiment of the invention is explained with reference to drawings below. This authentication system is ** constituted with an ID card and an ID card authentication device. ID card 11, and ID card authentication device 13 and the lineblock diagram of ** are shown in drawing 1 and drawing 2, respectively. ID card 11 is provided with the photograph sticking section 21 on which a cardholder's photograph is stuck, and the magnetic stripe 23 which is the magnetic storage media of tape shape as shown in drawing 1. ID card authentication device 13 is provided with the image reading part 31, the card reader/writer 33 (card R/W), the feature extraction part 35, the control section 37, the indicator 38, and the input part 39 as shown in drawing 2.

[0020]The image reading part 31 comprises an image scanner etc., for example, reads the photograph (picture) stuck on the photograph sticking section 21 of ID card 11, and acquires image data. A card reader / writer 33 reads the data which the data to the magnetic stripe 23 writes in, or is memorized by the magnetic stripe 23. The feature extraction part 35 extracts the characteristic data for specifying the image data from the image data acquired from the image reading part 31. This extraction method is mentioned later.

[0021]The control section 37 checks the justification of the ID card 11 by comparing the data memorized by the magnetic stripe 23 with the characteristic data extracted from the photograph stuck on the photograph sticking section 21 of ID card 11 for attestation at the time of attestation of ID card 11. The control section 37 controls the ID card authentication device 13 whole. The indicator 38 displays the result of attestation of ID card 11, etc. The input part 39 is for a user or an administrator to input directions.

[0022]This system performs issue of ID card 11 and attestation of ID card 11. These processings are explained below. First, when publishing ID card 11, a user or an administrator sticks the photograph of those who should turn into an owner of the card on the photograph sticking section 21 of ID card 11, equips the image reading part 31 of ID card authentication device 13, and inputs card issuing directions from the input part 39. The control section 37 of ID card authentication device 13 answers the input of these card issuing directions, and starts card issuing processing. Card issuing processing is explained below with reference to the flow chart of drawing 3.

[0023]First, the control section 37 of ID card authentication device 13 directs reading of the picture of the photograph stuck on the photograph sticking section 21 of ID card 11 to the

image reading part 31. The image reading part 31 answers these directions, reads the picture of the photograph stuck on the photograph sticking section 21 of ID card 11, and generates image data, such as bit map data, by a predetermined conversion process, for example (Step S1, S2).

[0024]Next, the control section 37 extracts a characterizing portion from image data, and it directs it to the feature extraction part 35 so that characteristic data may be generated. The feature extraction part 35 answers these directions, performs extracting processing (feature extraction processing) of a characterizing portion to the bit map data generated from the image reading part 31, and generates characteristic data (Step S3). This feature extraction processing is processing for lessening data volume by extracting only the information about a predetermined characterizing portion from bit map data with much data volume. An example of this feature extraction processing is explained with reference to drawing 4.

[0025]First, from a user's picture (bit map data) acquired by the image reading part 31, the feature extraction part 35 identifies the position (the point A, B, and C of drawing 4) of a left eye, a right eye, and a mouth, and generates those positional intervals AB, BC, and CA, i.e., distance, as the 1st characteristic data. Next, the feature extraction part 35 identifies the starting point (points D and F) and the end point (points E and G) of a supercilium, and generates those positions as the 2nd characteristic data. Next, the feature extraction part 35 identifies the both-ends point (the point H, I, and J, K) of eyes, and generates those positions as the 3rd characteristic data. Thus, the feature extraction part 35 generates the 1st, 2nd, and 3rd characteristic data as feature extraction data, for example.

[0026]Next, the feature extraction part 35 transmits the notice of the purport that generation of characteristic data was completed to the control section 37. The control section 37 answers this notice and displays the message of the purport that it is required that card R/W33 should be equipped with ID card 11 on the indicator 38. A user or an administrator equips card R/W33 with ID card 11. The control section 37 directs to card R/W33 that the characteristic data generated by the feature extraction part 35 writes in ID card 11. Card R/W33 answers the directions from the control section 37, and writes characteristic data in the magnetic stripe 23 of ID card 11 with which card R/W33 was equipped (step S4). Issue of ID card 11 in which the characteristic data which specifies by this the photograph stuck on the photograph sticking section 21 was memorized by the magnetic stripe 23 is completed.

[0027]The characteristic data generated with the described method is data in which distance, a position, etc. are shown, and the data volume is dramatically small as compared with the data volume of the data which compressed conventional image data or image data. Therefore, an ID card is realizable using the magnetic storage medium etc. in which it is cheap and structure is easy.

[0028]In a scene to be attested [of a user], ID card 11 published from the above-mentioned

issue processing is attested from ID card authentication device 13 by comparing the characteristic data memorized by the photograph stuck on the photograph sticking section 21 of the ID card 11, and the magnetic stripe 23. This authenticating processing is explained with reference to drawing 5.

[0029]First, a user or an administrator equips the image reading part 31 of ID card authentication device 13 with ID card 11 for attestation, and inputs directions of the purport that attestation of this ID card 11 is required from the input part 39. The control section 37 answers the input of these directions, and directs loading of the picture of the photograph stuck on the photograph sticking section 21 of ID card 11 to the image reading part 31. The image reading part 31 answers these directions, reads the picture of the photograph stuck on the photograph sticking section 21 of ID card 11, and generates bit map data by a predetermined conversion process (Step S11, S12).

[0030]Next, the control section 37 is directed to the feature extraction part 35 so that characteristic data may be generated from the generated bit map data. The feature extraction part 35 answers these directions, performs feature extraction processing to the generated bit map data, and generates characteristic data (Step S13). This feature extraction processing is performed in the same procedure as the feature extraction processing at the time of the above-mentioned card issuing processing.

[0031]The control section 37 is directed to card R/W33 so that the characteristic data memorized by the magnetic stripe 23 of ID card 11 may be read. Card R/W33 answers these directions and reads characteristic data from the magnetic stripe 23 of ID card 11 (Step S14).

[0032]Next, the control section 37 compares the characteristic data acquired from the photograph stuck on the photograph sticking section 21 of ID card 11 with the characteristic data read from the magnetic stripe 23, and distinguishes whether they are in agreement (Step S15). When in agreement, the control section 37 considers that the ID card 11 is a normal card with which unjust processing is not carried out, for example, performs normal processing of the ID card 11 displaying the message of a normal purport (Step S16). When not in agreement, the control section 37 considers that the ID card 11 is an inaccurate card, and error handling of sounding alarm, displaying an error message is performed (Step S17).

[0033]Thus, the characteristic data memorized by the photograph stuck on the photograph sticking section 21 of ID card 11 and the magnetic stripe 23 can be compared, and the ID card forged unjustly can be detected.

[0034]In this authenticating processing, since a lot of image data is not compared like before but only the characteristic data (for example, code which shows distance, a position, etc.) acquired from the picture is compared, processing speed can be made more nearly high-speed than before.

[0035]The shape is arbitrary if it has the magnetic stripe which memorizes the photograph

sticking section on which the shape of the ID card in the above-mentioned explanation is not limited to a card, but a photograph is stuck, and the above-mentioned characteristic data. For example, it may realize as an authentication system provided with the passport provided with a photograph sticking section and a magnetic stripe for this invention, and the passport authentication device which performs the issue and attestation. Thereby, the forged inaccurate passport is detectable.

[0036]The object item of the feature extraction in feature extraction processing is not limited to the item (the interval of eyes, a nose, and a mouth, a start/end point of a supercilium, the both-ends point of eyes) used by the above-mentioned explanation, but is arbitrary. For example, it may be made to extract the feature using the color characteristic of a face, etc. It may be made to generate the feature extraction data which can specify a user more correctly by carrying out weighting to two or more items, respectively. In this case, for example, individual difference may enlarge weighting to the characteristic data for a large portion, and individual difference may make small weighting to the characteristic data for a small portion.

[0037]If specification of a user is possible for the object of feature extraction processing, it is not limited to a photograph but is arbitrary. For example, it may have a field which displays a user's fingerprint, a portrait, etc., and the ID card which wrote those feature extraction data in the magnetic stripe may be used.

[0038]The ID card authentication device of this invention cannot be based on a system for exclusive use, but can be realized using the usual computer system. for example, the medium (a floppy disk.) which stored the program for performing above-mentioned operation in the computer to which the image scanner, and the card reader/writer were connected By installing this program from CD-ROM etc., the ID card authentication device which performs above-mentioned processing can be constituted.

[0039]Communication media (medium which holds a program temporarily and fluidly like a communication line, a communication network, and a communications system) may be sufficient as the medium for supplying a program to a computer. For example, this program may be put up for the bulletin board (BBS) of a communication network, and this may be distributed via a network. And above-mentioned processing can be performed by starting this program and performing like other application programs under control of OS.

[0040]The operation program is distributed to an ID card authentication device in a network, and it may be made to delete the program after execution at the time of execution of feature extraction processing. ID card 11 can be prevented from an ID card authentication device being destroyed by the inaccurate person, and the feature extraction program memorized inside being wrested, and being forged by this, using this program. It is desirable to strengthen security, when distributing a program via a network, as mentioned above.

[0041]

[Effect of the Invention]As explained above, according to this invention, the characteristic data which extracted and generated the feature from the picture information which specifies a user is memorized to the magnetic storage part of the card for attestation, and the data read from the magnetic storage part and the data which carried out feature extraction and was generated from picture information are compared at the time of attestation. The wrong card forged by unjust change of picture information, such as **** of a photograph, thereby, for example is detectable. Since the data volume memorized on the card for attestation by extracting only the feature from picture information becomes a small quantity, the card for attestation is realizable using the storage in which it is cheap and structure is easy.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]It is a figure showing the composition of the ID card of the ID card authentication system concerning an embodiment of the invention.
[Drawing 2]It is a figure showing the composition of the ID card authentication device of the ID card authentication system concerning an embodiment of the invention.
[Drawing 3]It is a flow chart for explaining card issuing processing.
[Drawing 4]It is a figure for explaining feature extraction processing.
[Drawing 5]It is a flow chart for explaining authenticating processing.
[Description of Notations]
11 ID card
13 ID card authentication device
21 Photograph sticking section
23 Magnetic stripe
31 Image reading part
33 Card R/W
35 Feature extraction part
37 Control section
38 Indicator
39 Input part

[Translation done.]

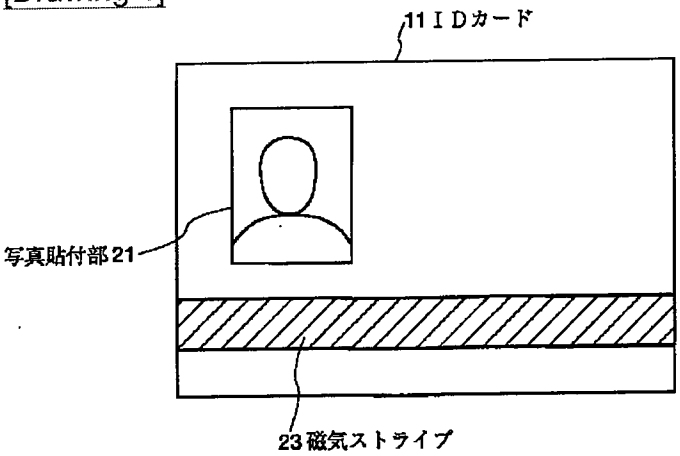
* NOTICES *

JPO and INPIT are not responsible for any
damages caused by the use of this translation.

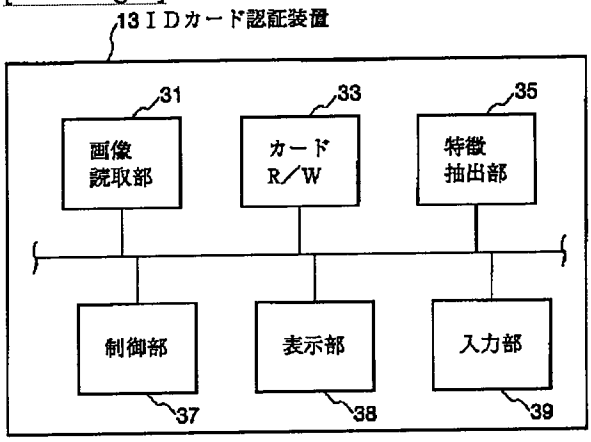
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

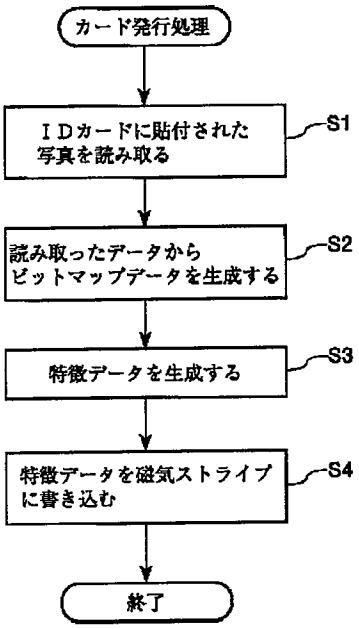
[Drawing 1]



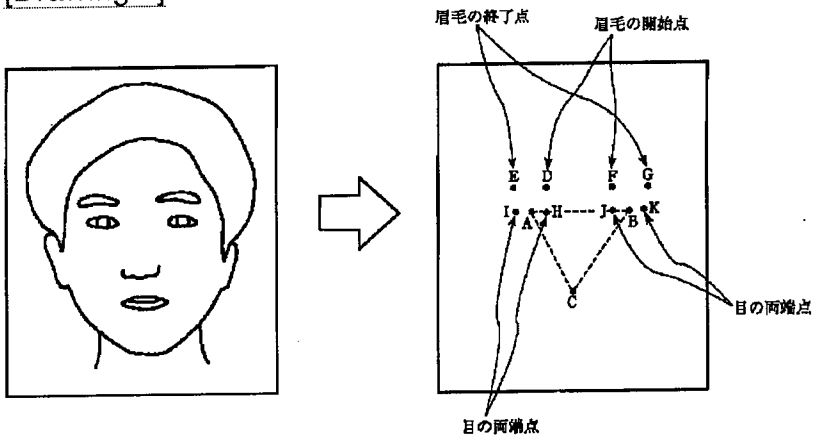
[Drawing 2]



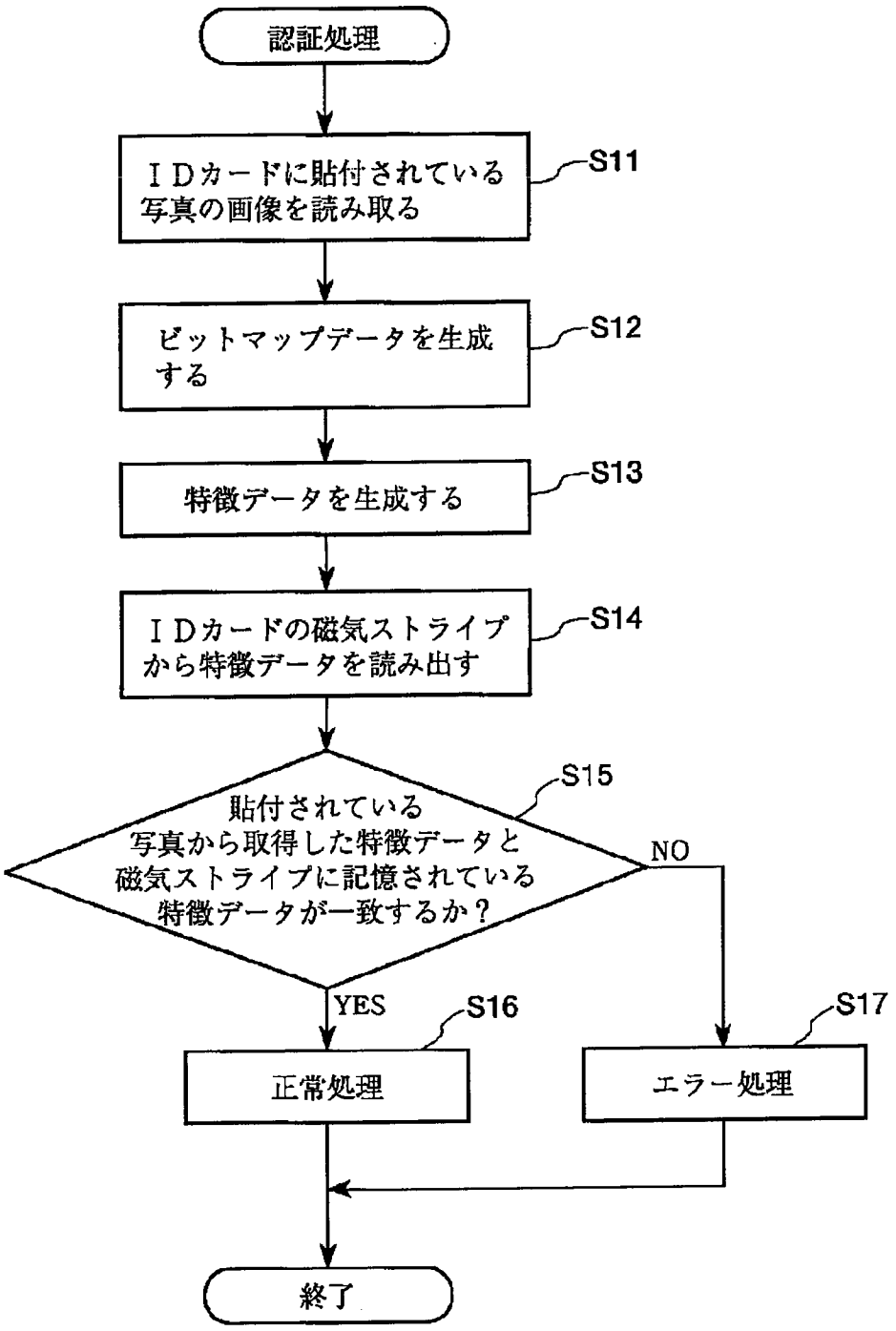
[Drawing 3]



[Drawing 4]



[Drawing 5]



[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（A）　(11)特許出願公開番号
特開平10－302034
(43)公開日　平成10年(1998)11月13日

(51)Int.Cl.[6]	識別記号	FI	
Ｇ０６Ｋ　17/00		Ｃ０６Ｋ　17/00	Ｔ
			Ａ
Ｇ０６Ｔ　7/00		Ｇ０６Ｆ　15/62	４６５Ｋ
Ｇ０６Ｋ　19/10		Ｇ０６Ｋ　19/00	Ｒ

審査請求　未請求　請求項の数６　ＯＬ　（全８頁）

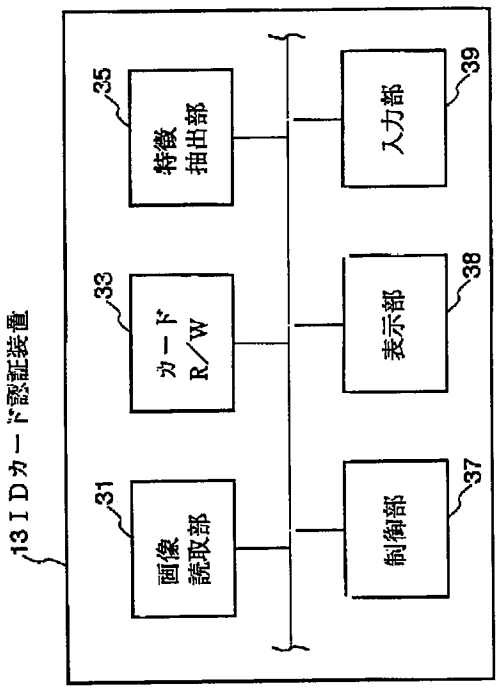
(21)出願番号　特願平9－107101

(22)出願日　平成９年(1997)４月24日

(71)出願人　000102728
株式会社エヌ・ティ・ティ・データ
東京都江東区豊洲三丁目３番３号
(72)発明者　荒川　弘熙
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(72)発明者　岩元　宏樹
東京都江東区豊洲三丁目３番３号　エヌ・ティ・ティ・データ通信株式会社内
(74)代理人　弁理士　木村　満

(54)【発明の名称】　認証システム、カード発行装置、認証装置、認証用カード及び認証方法

(57)【要約】
【課題】　偽造が困難であり、且つ、簡単で安価なＩＤカード及び該ＩＤカードを用いた認証システム及び方法を提供する。
【解決手段】　ＩＤカードは、利用者の写真を貼付するための写真貼付部と磁気ストライプとを備える。ＩＤカード発行時、ＩＤカード認証装置１３は、ＩＤカードに貼付されている写真の画像を読取り、特徴を抽出して生成した特徴データを磁気ストライプに記憶する。ＩＤカードの認証時、ＩＤカード認証装置１３は、ＩＤカードに貼付されている写真を読取り、特徴抽出を行って特徴データを生成し、予め磁気ストライプに記憶されている特徴データと比較する。比較した特徴データが一致する場合、ＩＤカード認証装置１３は、認証対象のＩＤカードを正常なカードと判別する。比較した特徴データが一致しない場合、ＩＤカード認証装置１３は、不正カードの検出処理を行う。



【特許請求の範囲】
【請求項１】利用者を特定する画像情報が表示され、記憶部を備える認証用カードと、該認証用カードを処理する認証装置と、を備える認証システムであって、
前記認証装置は、
前記認証用カードに表示されている前記画像情報を読み取る読取手段と、前記読取手段により読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出手段と、前記特徴データを前記記憶部に書き込む書込手段と、を備えるカード発行手段と、
認証時において、前記認証用カードに表示されている前記画像情報を前記読取手段により読み取り、前記特徴抽出手段により特徴データを生成する生成手段と、前記書込手段により前記認証用カードの前記記憶部に書き込まれている前記特徴データを読み出す読出手段と、前記読出手段より読み出された前記特徴データと、前記生成手段により生成された前記特徴データと、が一致するか否かを判別する判別手段と、前記読出手段より読み出された前記特徴データと、前記生成手段により生成された前記特徴データと、が一致しないと判別された場合、不正カードの検出を通知する手段と、を備える認証手段と、
を備えることを特徴とする認証システム。
【請求項２】利用者を特定する画像情報が表示され、記憶部を備える認証用カードを用いて利用者の認証を行う認証システムにおけるカード発行装置であって、
前記カード発行装置は、
前記認証用カードに予め表示されている前記画像情報を読み取る読取手段と、
前記読取手段により読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出手段と、
前記特徴データを前記記憶部に書き込む書込手段と、を備える、
ことを特徴とするカード発行装置。
【請求項３】利用者を特定する画像情報が表示され、該画像情報から特徴を抽出して生成した特徴データが記憶されている記憶部を備える認証用カードの認証を行う認証装置であって、
前記認証装置は、
前記認証用カードに表示されている前記画像情報を読み取る読取手段と、
前記読取手段により読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出手段と、
前記認証用カードの前記記憶部に書き込まれている前記特徴データを読み出す読出手段と、
前記読出手段により読み出された前記特徴データと、前記特徴抽出手段により生成された前記特徴データと、が一致するか否かを判別する判別手段と、
前記読出手段により読み出された前記特徴データと、前記特徴抽出手段により生成された前記特徴データと、が一致しないと判別された場合、不正カードの検出を通知する手段と、を備える、
ことを特徴とする認証装置。
【請求項４】利用者の認証を行う認証システムにおいて使用される認証用カードであって、
前記認証用カードは、
利用者を特定する画像情報を表示する表示領域と、
前記表示領域に表示されている前記画像情報から特徴を抽出して生成された特徴データを記憶する記憶領域と、を備える、
ことを特徴とする認証用カード。
【請求項５】利用者を特定する画像情報が表示され、記憶部を備える認証用カードを用いて利用者の認証を行う認証方法であって、
前記認証用カードに予め表示されている前記画像情報を読み取る読取ステップと、
読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出ステップと、
前記特徴抽出ステップより生成された前記特徴データを前記認証用カードの前記記憶部に記憶する記憶ステップと、
を備えることを特徴とする認証方法。
【請求項６】利用者を特定する画像情報が表示され、該画像情報から特徴を抽出して生成した特徴データが記憶されている記憶部を備える認証用カードを用いて利用者の認証を行う認証方法であって、
前記認証用カードに予め表示されている前記画像情報を読み取る読取ステップと、
前記読取ステップにより読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出ステップと、
前記認証用カードの前記記憶部に予め記憶されている前記特徴データを読み出す読出ステップと、
前記読出ステップにより読み出された前記特徴データと、前記特徴抽出ステップにより生成された前記特徴データと、が一致するか否かを判別する判別ステップと、
前記読出ステップにより読み出された前記特徴データと、前記特徴抽出ステップにより生成された前記特徴データと、が一致しないと判別された場合、不正カードの検出を通知するステップと、
を備えることを特徴とする認証方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】本発明は、利用者の認証を行う認証システムに関する。
【０００２】
【従来の技術】利用者の写真が貼付されているＩＤカード等を用いた認証システムでは、貼付されている写真が不正に貼り替えられていないことを確認する必要がある。このため、例えば、貼付された写真の画像データをＩＤカードに記憶し、それらを照合することにより認証

を行う認証システムが提案されている。

【0003】

【発明が解決しようとする課題】このようなシステムでは、ＩＤカードに記憶されるデータとして、例えば、貼付された写真の画像データを使用するシステムが提案されている。この場合、データ量が多大な為、磁気ストライプ等の記憶容量の小さい記憶媒体を用いることは不可能であり、大容量のＩＣ（Integrated Circuit）メモリを用いる必要があった。

【0004】このため、写真の画像データを圧縮し、データ量を小さくした圧縮データをＩＤカードに記憶するシステムも提案されている。しかし、この場合、その認証処理において、予めカードに記憶されている圧縮データを伸張したデータと、貼付されている写真の画像データと、が一致していることを確認することは実質上困難であるという問題があった。なぜなら、圧縮して伸張したデータは、圧縮前のデータとは完全に一致しない場合が多いからである。

【0005】この対策案として、例えば、特開平８－１２９６３４には、認証時に、貼付されている写真を読取り、予めカードに記憶されている圧縮データと同一の手順で圧縮し、更に伸張を行い、その結果得られたデータと、カードに記憶されている圧縮データを伸張したデータと、を照合するシステムが提案されている。しかし、この場合、認証時に、カードに記憶されているデータを伸張すると共に、カードに貼付されている写真の画像データを圧縮し、伸張しなければならず、レスポンスが遅くなるという問題がある。

【0006】本発明は、上記実状に鑑みてなされたもので、偽造が困難であり、且つ、構成が簡単で安価なＩＤカード及び該ＩＤカードを用いた認証システム、装置及び方法を提供することを目的とする。さらにこれらに用いて好適なカード発行装置及び認証用カードを提供することを他の目的とする。

【0007】

【課題を解決するための手段】上記目的を達成するため、この発明の第１の観点に係る認証システムは、利用者を特定する画像情報が表示され、記憶部を備える認証用カードと、該認証用カードを処理する認証装置と、を備える認証システムであって、前記認証装置は、前記認証用カードに表示されている前記画像情報を読み取る読取手段と、前記読取手段により読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出手段と、前記特徴データを前記記憶部に書き込む書込手段と、を備えるカード発行手段と、認証時において、前記認証用カードに表示されている前記画像情報を前記読取手段により読み取り、前記特徴抽出手段により特徴データを生成する生成手段と、前記書込手段より前記認証用カードの前記記憶部に書き込まれている前記特徴データを読み出す読出手段と、前記読出手段より読み出された前記特徴データと、前記生成手段により生成された前記特徴データと、が一致するか否かを判別する判別手段と、前記読出手段より読み出された前記特徴データと、前記生成手段により生成された前記特徴データと、が一致しないと判別された場合、不正カードの検出を通知する手段と、を備える認証手段と、を備える。

【0008】このような構成によれば、利用者を特定する画像情報から特徴を抽出して生成した特徴データを記憶部に記憶し、認証時に、記憶部から読み出したデータと、画像情報から特徴抽出して生成したデータと、を照合する。これにより、例えば、写真の貼替等の画像情報の不正な変更により偽造された不正カードを検出することができる。また、画像情報から特徴のみを抽出することにより、カードに記憶するデータ量が少量となるため、安価で構造が簡単な磁気記憶媒体等を用いて認証用カードを実現することができる。

【0009】また、この発明の第２の観点に係るカード発行装置は、利用者を特定する画像情報が表示され、記憶部を備える認証用カードを用いて利用者の認証を行う認証システムにおけるカード発行装置であって、前記カード発行装置は、前記認証用カードに予め表示されている前記画像情報を読み取る読取手段と、前記読取手段により読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出手段と、前記特徴データを前記記憶部に書き込む書込手段と、を備える。

【0010】このような構成によれば、利用者を特定する画像情報から特徴を抽出して生成した特徴データを認証時における照合用データとして記憶部に記憶する。これにより、例えば、写真の貼替等の画像情報の不正な変更によるカードの偽造を防止することができる。また、画像情報から特徴のみを抽出することにより、カードに記憶するデータ量が少量となるため、安価で構造が簡単な磁気記憶媒体等を用いて認証用カードを実現することができる。

【0011】また、この発明の第３の観点に係る認証装置は、利用者を特定する画像情報が表示され、該画像情報から特徴を抽出して生成した特徴データが記憶されている記憶部を備える認証用カードの認証を行う認証装置であって、前記認証装置は、前記認証用カードに予め表示されている前記画像情報を読み取る読取手段と、前記読取手段により読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出手段と、前記認証用カードの前記記憶部に書き込まれている前記特徴データを読み出す読出手段と、前記読出手段により読み出された前記特徴データと、前記特徴抽出手段により生成された前記特徴データと、が一致するか否かを判別する判別手段と、前記読出手段により読み出された前記特徴データと、前記特徴抽出手段により生成された前記特徴データと、が一致しないと判別された場合、不正カードの検出を通知する手段と、を備える。

【0012】このような構成によれば、カード認証時に、記憶部から読み出した予め特徴を抽出して生成されたデータと、画像情報から特徴抽出して生成したデータと、を照合する。これにより、例えば、写真の貼替等の画像情報の不正な変更により偽造された不正カードを検出することができる。

【0013】また、この発明の第４の観点に係る認証用カードは、利用者の認証を行う認証システムにおいて使用される認証用カードであって、前記認証用カードは、利用者を特定する画像情報を表示する表示領域と、前記表示領域に表示されている前記画像情報から特徴を抽出して生成された特徴データを記憶する記憶領域と、を備える。

【0014】このような構成によれば、該認証用カードは、利用者を特定する画像情報から特徴を抽出して生成した特徴データを認証時の照合用データとして記憶するための記憶領域を備える。これにより、例えば、写真の貼替等の画像情報の不正な変更によるカードの偽造を防止することができる。また、画像情報から特徴のみを抽出することにより、カードに記憶するデータ量が少量となるため、構造が簡単な記憶媒体等を用いて認証用カードを実現することができる。

【0015】また、この発明の第５の観点に係る認証方法は、利用者を特定する画像情報が表示され、記憶部を備える認証用カードを用いて利用者の認証を行う認証方法であって、前記認証用カードに表示されている前記画像情報を読み取る読取ステップと、読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出ステップと、前記特徴抽出ステップより生成された前記特徴データを前記認証用カードの前記記憶部に記憶する記憶ステップと、を備える。

【0016】このような構成によれば、利用者を特定する画像情報から特徴を抽出して生成した特徴データを認証時における照合用データとして認証用カードの記憶部に記憶する。これにより、例えば、写真の貼替等の画像情報の不正な変更によるカードの偽造を防止することができる。また、画像情報から特徴のみを抽出することにより、カードに記憶するデータ量が少量となるため、安価で構造が簡単な記憶媒体等を用いて認証用カードを実現することができる。

【0017】また、この発明の第６の観点に係る認証方法は、利用者を特定する画像情報が表示され、該画像情報から特徴を抽出して生成した特徴データが記憶されている記憶部を備える認証用カードを用いて利用者の認証を行う認証方法であって、前記認証用カードに予め表示されている前記画像情報を読み取る読取ステップと、前記読取ステップにより読み取られた前記画像情報から特徴を抽出し、特徴データを生成する特徴抽出ステップと、前記認証用カードの前記記憶部に予め記憶されている前記特徴データを読み出す読出ステップと、前記読出ステップにより読み出された前記特徴データと、前記特徴抽出ステップにより生成された前記特徴データと、が一致するか否かを判別する判別ステップと、前記読出ステップにより読み出された前記特徴データと、前記特徴抽出ステップにより生成された前記特徴データと、が一致しないと判別された場合、不正カードの検出を通知するステップと、を備える。

【0018】このような構成によれば、カード認証時に、記憶部から読み出した予め特徴を抽出して生成されたデータと、画像情報から特徴抽出して生成したデータと、を照合する。これにより、例えば、写真の貼替等の画像情報の不正な変更により偽造された不正カードを検出することができる。

【0019】

【発明の実施の形態】本発明の実施の形態にかかる認証システムについて、以下図面を参照して説明する。この認証システムは、ＩＤカードと、ＩＤカード認証装置と、から構成される。ＩＤカード１１と、ＩＤカード認証装置１３と、の構成図をそれぞれ図１、図２に示す。ＩＤカード１１は、図１に示すように、カード所有者の写真が貼付される写真貼付部２１と、テープ状の磁気記憶媒体である磁気ストライプ２３と、を備える。ＩＤカード認証装置１３は、図２に示すように、画像読取部３１と、カードリーダ／ライタ（カードＲ／Ｗ）３３と、特徴抽出部３５と、制御部３７と、表示部３８と、入力部３９と、を備える。

【0020】画像読取部３１は、例えばイメージスキャナ等から構成され、ＩＤカード１１の写真貼付部２１に貼付された写真（画像）を読取り、画像データを取得する。カードリーダ／ライタ３３は、磁気ストライプ２３へのデータの書き込み、又は、磁気ストライプ２３に記憶されているデータの読み込みを行う。特徴抽出部３５は、画像読取部３１より取得された画像データから、その画像データを特定するための特徴データを抽出する。この抽出方法については後述する。

【0021】制御部３７は、ＩＤカード１１の認証時に、磁気ストライプ２３に記憶されているデータと認証対象のＩＤカード１１の写真貼付部２１に貼付されている写真から抽出された特徴データとを比較することにより、そのＩＤカード１１の正当性をチェックする。また、制御部３７は、ＩＤカード認証装置１３全体を制御する。表示部３８は、ＩＤカード１１の認証の結果等を表示する。入力部３９は、利用者又は管理者が指示を入力するためのものである。

【0022】本システムは、ＩＤカード１１の発行と、ＩＤカード１１の認証と、を行う。これらの処理について、以下説明する。まず、ＩＤカード１１を発行する場合、利用者又は管理者は、ＩＤカード１１の写真貼付部２１にそのカードの所有者となるべき者の写真を貼付し、ＩＤカード認証装置１３の画像読取部３１に装着

し、入力部３９からカード発行指示を入力する。ＩＤカード認証装置１３の制御部３７は、このカード発行指示の入力に応答して、カード発行処理を開始する。カード発行処理について、図3のフローチャートを参照して、以下説明する。

【００２３】まず、ＩＤカード認証装置１３の制御部３７は、ＩＤカード１１の写真貼付部２１に貼付されている写真の画像の読取を画像読取部３１に指示する。画像読取部３１は、この指示に応答し、ＩＤカード１１の写真貼付部２１に貼付されている写真の画像を読み取り、所定の変換処理により、例えば、ビットマップデータ等の画像データを生成する（ステップＳ１、Ｓ２）。

【００２４】次に、制御部３７は、画像データから特徴部分を抽出し、特徴データを生成するよう、特徴抽出部３５に指示する。特徴抽出部３５は、この指示に応答して、画像読取部３１より生成されたビットマップデータに対して特徴部分の抽出処理（特徴抽出処理）を行い、特徴データを生成する（ステップＳ３）。この特徴抽出処理は、データ量の多いビットマップデータから所定の特徴部分に関する情報のみを抽出することにより、データ量を少なくするための処理である。この特徴抽出処理の一例について、図４を参照して説明する。

【００２５】まず、特徴抽出部３５は、画像読取部３１により取得された利用者の画像（ビットマップデータ）から、左目と右目と口との位置（図４の点Ａ、Ｂ、Ｃ）を識別し、それらの位置間隔、即ち、距離ＡＢ、ＢＣ、ＣＡを第１の特徴データとして生成する。次に、特徴抽出部３５は、眉毛の開始点（点Ｄ、Ｆ）及び終了点（点Ｅ、Ｇ）を識別し、それらの位置を第２の特徴データとして生成する。次に、特徴抽出部３５は、目の両端点（点Ｈ、Ｉ、Ｊ、Ｋ）を識別し、それらの位置を第３の特徴データとして生成する。このようにして、特徴抽出部３５は、例えば、第１、第２、第３の特徴データを特徴抽出データとして生成する。

【００２６】次に、特徴抽出部３５は、特徴データの生成が完了した旨の通知を制御部３７に送信する。制御部３７は、この通知に応答して、ＩＤカード１１をカードＲ／Ｗ３３に装着することを要求する旨のメッセージを表示部３８に表示する。利用者又は管理者は、ＩＤカード１１をカードＲ／Ｗ３３に装着する。また、制御部３７は、特徴抽出部３５により生成された特徴データをＩＤカード１１に書き込むようカードＲ／Ｗ３３に指示する。カードＲ／Ｗ３３は、制御部３７からの指示に応答し、カードＲ／Ｗ３３に装着されたＩＤカード１１の磁気ストライプ２３に特徴データを書き込む（ステップＳ４）。これにより、写真貼付部２１に貼付された写真を特定する特徴データが磁気ストライプ２３に記憶されたＩＤカード１１の発行が完了する。

【００２７】なお、上記方法で生成された特徴データは、距離や位置等を示すデータであり、そのデータ量は、従来の画像データ又は画像データを圧縮したデータのデータ量と比較して非常に小さい。よって、安価で構造が簡単な磁気記憶媒体等を用いてＩＤカードを実現することができる。

【００２８】上記発行処理より発行されたＩＤカード１１は、利用者の認証が必要な場面において、ＩＤカード認証装置１３より、そのＩＤカード１１の写真貼付部２１に貼付された写真と磁気ストライプ２３に記憶された特徴データとが照合されることにより認証される。この認証処理について、図５を参照して説明する。

【００２９】まず、利用者又は管理者が、認証対象のＩＤカード１１をＩＤカード認証装置１３の画像読取部３１に装着し、入力部３９より該ＩＤカード１１の認証を要求する旨の指示を入力する。制御部３７は、この指示の入力に応答して、ＩＤカード１１の写真貼付部２１に貼付されている写真の画像の読込を画像読取部３１に指示する。画像読取部３１は、この指示に応答し、ＩＤカード１１の写真貼付部２１に貼付されている写真の画像を読み取り、所定の変換処理により、ビットマップデータを生成する（ステップＳ１１、Ｓ１２）。

【００３０】次に、制御部３７は、生成したビットマップデータから特徴データを生成するよう、特徴抽出部３５に指示する。特徴抽出部３５は、この指示に応答して、生成されたビットマップデータに対して特徴抽出処理を行い、特徴データを生成する（ステップＳ１３）。なお、この特徴抽出処理は上記カード発行処理時における特徴抽出処理と同様の手順にて実行される。

【００３１】また、制御部３７は、ＩＤカード１１の磁気ストライプ２３に記憶されている特徴データを読み出すよう、カードＲ／Ｗ３３に指示する。カードＲ／Ｗ３３は、この指示に応答して、ＩＤカード１１の磁気ストライプ２３から特徴データを読み出す（ステップＳ１４）。

【００３２】次に、制御部３７は、ＩＤカード１１の写真貼付部２１に貼付されている写真から取得した特徴データと、磁気ストライプ２３から読み出した特徴データと、を比較し、それらが一致するか否かについて判別する（ステップＳ１５）。一致する場合、制御部３７は、そのＩＤカード１１を、不正な加工がされていない正常なカードであるとみなし、例えば、そのＩＤカード１１が正常である旨のメッセージを表示する等の正常処理を行う（ステップＳ１６）。また、一致しない場合、制御部３７は、そのＩＤカード１１を不正なカードとみなし、アラームを鳴らす、エラーメッセージを表示する、等のエラー処理を行う（ステップＳ１７）。

【００３３】このようにして、ＩＤカード１１の写真貼付部２１に貼付されている写真と磁気ストライプ２３に記憶されている特徴データとを照合し、不正に偽造されたＩＤカードを検出することができる。

【００３４】なお、この認証処理では、従来のように大

量の画像データを比較するのではなく、画像から取得した特徴データ（例えば、距離、位置、等を示すコード）のみを比較するため、処理速度を従来よりも高速にすることができる。

【００３５】なお、上記説明におけるＩＤカードの形状はカードに限定されず、写真が貼付される写真貼付部と上記特徴データを記憶する磁気ストライプとを備えていれば、その形状は任意である。例えば、本発明を、写真貼付部と磁気ストライプとを備えるパスポートと、その発行及び認証を行うパスポート認証装置と、を備える認証システムとして実現してもよい。これにより、偽造された不正なパスポートを検出することができる。

【００３６】なお、特徴抽出処理における特徴抽出の対象項目は、上記説明で使用した項目（目と鼻と口の間隔、眉毛の開始／終了点、目の両端点）に限定されず任意である。例えば、顔の色特性、等を利用してその特徴を抽出するようにしてもよい。また、複数の項目に対してそれぞれ重み付けをすることにより、より正確に利用者を特定できる特徴抽出データを生成するようにしてもよい。この場合、例えば、個人差が大きい部分を対象とした特徴データに対する重み付けを大きくし、個人差が小さい部分を対象とした特徴データに対する重み付けを小さくしてもよい。

【００３７】また、特徴抽出処理の対象は、利用者を特定可能であれば、写真に限定されず、任意である。例えば、利用者の指紋、似顔絵、等を表示する領域を備え、それらの特徴抽出データを磁気ストライプに書き込んだＩＤカードを用いてもよい。

【００３８】なお、この発明のＩＤカード認証装置は、専用のシステムによらず、通常のコンピュータシステムを用いて実現可能である。例えば、イメージスキャナとカードリーダ／ライタとが接続されたコンピュータに上述の動作を実行するためのプログラムを格納した媒体（フロッピーディスク、ＣＤ－ＲＯＭ等）から該プログラムをインストールすることにより、上述の処理を実行するＩＤカード認証装置を構成することができる。

【００３９】また、コンピュータにプログラムを供給するための媒体は、通信媒体（通信回線、通信ネットワーク、通信システムのように、一時的且つ流動的にプログラムを保持する媒体）でもよい。例えば、通信ネットワークの掲示板（ＢＢＳ）に該プログラムを掲示し、これをネットワークを介して配信してもよい。そして、このプログラムを起動し、ＯＳの制御下で、他のアプリケーションプログラムと同様に実行することにより、上述の処理を実行することができる。

【００４０】また、特徴抽出処理の実行時に、その動作プログラムをネットワークでＩＤカード認証装置に配布し、実行後、そのプログラムを削除するようにしてもよい。これにより、不正者によって、ＩＤカード認証装置が破壊され、内部に記憶された特徴抽出プログラムが奪取され、該プログラムを用いてＩＤカード１１が偽造されることを防止することができる。なお、上述したようにネットワークを介してプログラムを配布する場合は、セキュリティを強化することが望ましい。

【００４１】

【発明の効果】以上説明したように、本発明によれば、利用者を特定する画像情報から特徴を抽出して生成した特徴データを認証用カードの磁気記憶部に記憶し、認証時に、磁気記憶部から読み出したデータと、画像情報から特徴抽出して生成したデータと、を照合する。これにより、例えば、写真の貼替等の画像情報の不正な変更により偽造された不正カードを検出することができる。また、画像情報から特徴のみを抽出することにより、認証用カードに記憶するデータ量が少量となるため、安価で構造が簡単な記憶媒体を用いて認証用カードを実現することができる。

【図面の簡単な説明】

【図１】本発明の実施の形態に係るＩＤカード認証システムのＩＤカードの構成を示す図である。

【図２】本発明の実施の形態に係るＩＤカード認証システムのＩＤカード認証装置の構成を示す図である。

【図３】カード発行処理を説明するためのフローチャートである。

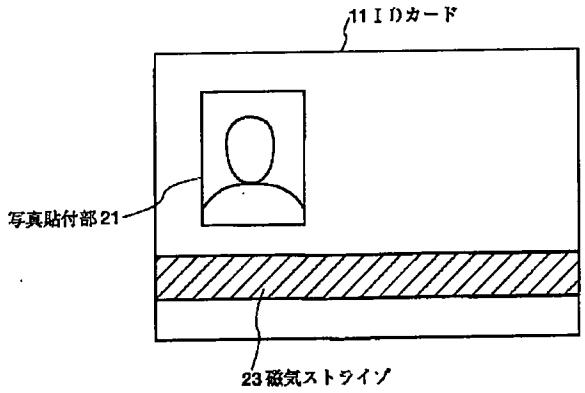
【図４】特徴抽出処理を説明するための図である。

【図５】認証処理を説明するためのフローチャートである。

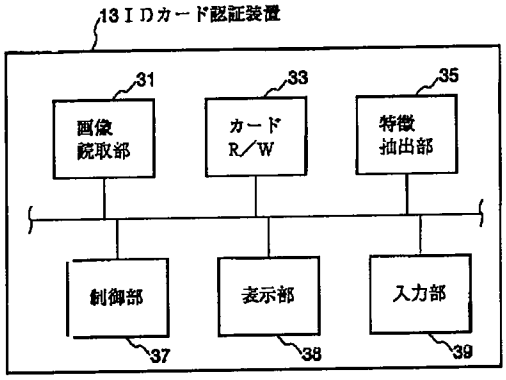
【符号の説明】

１１　ＩＤカード
１３　ＩＤカード認証装置
２１　写真貼付部
２３　磁気ストライプ
３１　画像読取部
３３　カードＲ／Ｗ
３５　特徴抽出部
３７　制御部
３８　表示部
３９　入力部

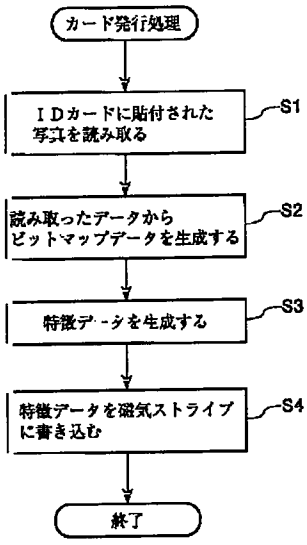
【図１】


11ＩＤカード
写真貼付部21
23磁気ストライプ

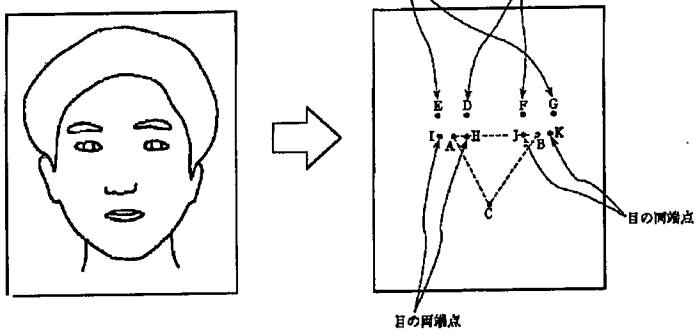
【図２】


13ＩＤカード認証装置
31
画像
読取部
33
カード
R／W
35
特徴
抽出部
制御部
表示部
入力部
37
38
39

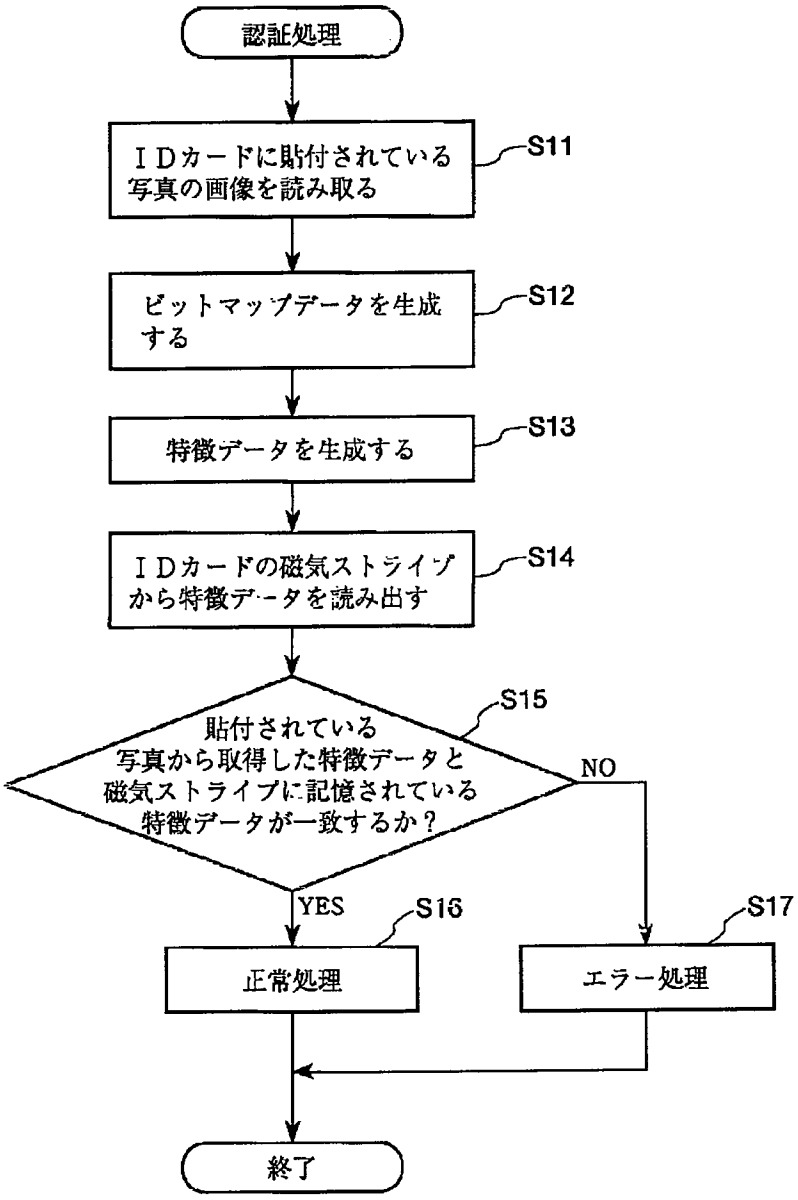
【図３】


カード発行処理
ＩＤカードに貼付された
写真を読み取る
S1
読み取ったデータから
ビットマップデータを生成する
S2
特徴データを生成する
S3
特徴データを磁気ストライプ
に書き込む
S4
終了

【図４】


眉毛の終了点
眉毛の開始点
E
D
F
G
I
A
H
J
B
K
C
目の両端点
目の両端点

【図5】


認証処理
ＩＤカードに貼付されている写真の画像を読み取る
S11
ビットマップデータを生成する
S12
特徴データを生成する
S13
ＩＤカードの磁気ストライプから特徴データを読み出す
S14
貼付されている写真から取得した特徴データと磁気ストライプに記憶されている特徴データが一致するか？
S15
NO
YES
S16
正常処理
S17
エラー処理
終了